



## PARLIAMENTARY BRIEFING: GROK - JANUARY 2026

---

*The Online Safety Act Network comprises over 70 organisations, campaigners and academics with a longstanding interest in the Online Safety Act. Our interests span the whole range of online harms: child protection, terrorism, extremism, violence against women and girls, suicide and self-harm prevention, mental health, online abuse, fraud and scams, mis- and disinformation, harms to democracy and threats to our information environment.*

### **What happened?**

Over the last two weeks there have been numerous reports of women and children being “undressed”, or portrayed in sexualised positions, by the image-generation function in Grok, the AI chatbot embedded in X, Grok. The chatbot, if prompted, can create multiple versions of the image with the person in sexual poses, covered in blood or white liquid, demeaned and dehumanised. Figures last week [from Bloomberg](#) suggested that 6000 such images were being produced every hour. The Internet Watch Foundation on Wednesday [found examples](#) of category C child sexual abuse material produced by the standalone Grok app on the dark web. [According to Wired](#), that tool, Grok Imagine, is creating even more graphic content than that found on X.

Concerns have been raised since [at least June of last year](#) about its use to create “undressed” images of women and children. What changed in recent weeks is the introduction of the ability by users to ask for images posted by other people on X to be edited, which has removed friction and contributed to the deluge of non-consensual, sexually explicit images on the platform. However, given that X has been aware of this issue for some time, they have clearly failed to carry out a proper risk assessment as required by the Online Safety Act.

X announced last week that the functionality will now only be available to paid subscribers. However, this effectively means that X is monetising the creation of CSAM and non-consensual intimate images rather than stopping it happening in the first place. The Government rightly described this update from X as “insulting” to victims of misogyny and sexual violence, following that the change “simply turns an AI feature that allows the creation of unlawful images into a premium service”.

### **What are regulators doing?**

The announcement made on Monday is the first formal step in enforcing the Online Safety Act (OSA) duties. As outlined in Professor Lorna Woods' analysis, [which you can read in full here](#), Ofcom are now at the stage of analysing the evidence gathered. This will include evidence arising from their contact with X on 5th January to which the platform responded on the 10th January. Once this information has been analysed - and if Ofcom determines that there has been a compliance failure - the OSA specifies that Ofcom should issue a [provisional notice](#) and specify a time within which the service provider should respond and make representations. It is then that Ofcom can issue the final notice of contravention.

### ***What needs to happen next?***

We welcomed [SoS Liz Kendall's statement](#) in the Commons on Monday announcing that the new offences for deepfake abuse in the Data (Use and Access) Act will come into force this week, as well as the addition of deepfake abuse to the list of priority offences in the Online Safety Act. Yet there is more that can be done to ensure that platforms are not able to let abuse occur on their site in the first place.

Whilst the Government awaits action from the regulator, Ofcom, urgent action is needed to fill the holes in the Online Safety Act which have led to Ofcom creating a weak set of codes of practice, limiting their powers to take action on X, despite the unacceptable levels of harm being caused at scale to women and girls. This includes:

- Strengthening existing laws to make sure that chatbots are covered: at present, the Online Safety Act only provides partial coverage. The Government could urgently bring an amendment in through the Crime and Policing Bill to rectify this. (Here's our explainer on [chatbots](#).)
- Convert the Ofcom OSA guidance for protection of women and girls into a code of practice that can be enforceable. Musk's actions have shown he cares little about protecting women - voluntary guidance is not going to change that.
- Strengthen the obligation in the Act that regulated services take reasonable steps to seek to reduce the risk of harm to users as identified in their OSA risk assessments.
- Revise the "clear and detailed" and "technically feasible" conditions for code of practice measures to allow for more stretching, outcome-focused measures in the OSA codes.
- Remove the safe harbour provision.
- Insert a definition of safety by design into the Act to make clear to Ofcom and services what Parliament intended, and lay secondary legislation to require Ofcom to produce a "safety by design" code of practice, a cross-cutting code to sit beneath the existing codes. This should also clarify the requirement that services address harms to children caused by addictive or compulsive design.
- Make clear that, once illegal content or imagery has been removed, further shares of the same material are removed without further moderation requirements: a 'stay-down' provision.
- Set a minimum standard for Terms of Service (ToS) for category 1 platforms and include a "no rolling back" requirement such that ToS and safety measures must be maintained to an equivalent or greater protection to that at the time of OSA Royal Assent.

To ensure that victims have proper access to redress, the Government must support the amendment from Baroness Owen in the Crime and Policing Bill to make it mandatory for platforms to take down intimate images when reported to them within 48 hours. (This mirrors the US Take It Down Act.)

Furthermore, the Government should lead by example by taking its own accounts off X (or at the very least stop using them as their priority comms channel), as we have outlined in our [letter to the Prime Minister](#), which was co-signed by a number of VAWG sector organisations and experts.

***It is vital that the Government does not wait for another scandal to take this issue seriously. Whilst the Online Safety Act provides a solid framework, the steps laid out above would ensure that platforms do not continue to prioritise profits over user safety. We would welcome the opportunity to discuss this further with you.***